



**TRICARE Management Activity (TMA)**

**Baseline Administrative Simplification Integrated Compliance Solution  
(HIPAA BASICS™)**

**Training Reference: Regular User Manual  
Version 1.0**

**Prepared By:  
Booz Allen Hamilton**

*This document contains proprietary information and will be handled within Government regulations.  
It is intended solely for the use and information of the Military Health System.*

## Table of Contents

1.0	INTRODUCTION .....	1
1.1	ABOUT HIPAA BASICS™ .....	1
1.2	SYSTEM REQUIREMENTS .....	1
1.3	PASSWORD REQUIREMENTS.....	1
1.4	GETTING STARTED.....	2
1.5	SUBSCRIPTIONS AND USER TYPES .....	2
1.5.1	SUBSCRIBER ADMINISTRATOR.....	2
1.5.2	LEAD USERS .....	3
1.5.3	REGULAR USERS .....	3
2.0	ACCESSING HIPAA BASICS™ .....	3
2.1	MAIN MENU SCREEN.....	5
2.1.1	TITLE MENU .....	6
2.1.2	APPLICATION MENU.....	7
2.1.3	APPLICATION WINDOW.....	7
2.2	DEMO GAP .....	7
3.0	ANSWERING REQUIRMENTS AND TASKS .....	8
4.0	TECHNICAL SUPPORT .....	12
4.1	SYSTEMS MAINTENANCE .....	12
4.2	INFORMATION UPDATES.....	13
4.3	VERSION UPGRADES .....	13
4.4	TMA HIPAA SUPPORT CENTER.....	13
5.0	GLOSSARY .....	14

## Documentation Configuration Control

This page lists all of the changes that have been made to the HIPAA BASICS™ Regular User Manual throughout its development.

Version	Release Date	Summary of Changes

## 1.0 INTRODUCTION

HIPAA BASICS™ is a proprietary online application that is accessible to authorized users via a Web browser. This section of the HIPAA BASICS™ Subscriber Administrator Manual identifies the intent of HIPAA BASICS™, the requirements for accessing HIPAA BASICS™, and BASICS™ user responsibilities (identified by user type).

### 1.1 About HIPAA BASICS™

HIPAA BASICS™ provides access to regulatory requirements and tasks; helps assess HIPAA compliance status, assists tracking and reporting, and project planning. It is specifically designed for those who have responsibilities in assessing and implementing compliance with the regulations relating to the Health Insurance Portability Administration Act of 1996 Administrative Simplification. HIPAA BASICS™ allows users to conduct online HIPAA compliance assessments, status reports, gap analysis reports, and generate and download project plans that are based on these assessments.

### 1.2 System Requirements

The HIPAA BASICS™ application has the following user hardware and software requirements.

#### **Hardware:**

- IBM Compatible PC with Intel P-350 processor (or better) with 64 MB (or higher) RAM
- Mouse or pointing device

#### **Software:**

- Microsoft Internet Explorer v5.0 (or higher)
- Notepad
- Adobe Acrobat Reader 5+
- Microsoft Project 2000 or Microsoft Excel

#### **Settings:**

The PC should be configured to access the TMA network

### 1.3 Password Requirements

The following identifies all of the password requirements for HIPAA BASICS™. All users need to be aware of these requirements when creating and/or changing passwords.

Passwords must be 8-15 characters long and contain characters from all four of the following classes:

- English upper case and lower case letters
- Arabic numerals (0, 1, 2, ...9)
- Non alphanumeric special characters (!, @, \$, %, \*,...)
- Cannot contain user first and last name OR subscriber name

Passwords will expire after 90 days

- User will be prompted to change password
- Cannot be reused within 5 password changes

Force change of password upon first login and after password reset by the HIPAA Support Center or your Subscriber Administrator

- Users will be locked out after three unsuccessful login attempts
- Users must contact their Subscriber Administrator to have their account unlocked

Password security

- Single characters cannot be repeated more than twice in password

## 1.4 Getting Started

Access control within the HIPAA BASICS™ application is provided through Subscriptions and unique User IDs and Passwords.

Users require a valid account with a user ID and password in order to access HIPAA BASICS™. Subscriber Administrators are responsible for setting up and maintaining user accounts within their Subscription. In order for a Subscriber Administrator account to be created, Service Representatives must route an approved request for the creation of a Subscriber Administrator account to the TMA HIPAA Support Center. Once the approved request has been processed, the TMA HIPAA Support Center will send two emails to the Subscriber Administrator, identifying their Subscription, User Id, and password.

## 1.5 Subscriptions and User Types

There are three classes of user accounts that exist within the HIPAA BASICS™ application: Subscriber Administrator, Lead User, and Regular User account. Each of these user accounts resides within a defined Subscription.

The Subscription refers to the organization that has a license for HIPAA BASICS™ at their Military Treatment Facility (MTF). The Subscription is used in conjunction with the user ID and password to gain access to the HIPAA BASICS™ application. Subscriptions are created by the HIPAA Support Center at the discretion of the Service Representative. A description of the user types is provided in the following subsections.

### 1.5.1 Subscriber Administrator

The Subscriber Administrator manages the HIPAA BASICS™ user accounts within the MTF and its freestanding clinics. The Subscriber Administrator sets up users, provides user IDs and passwords, adds and modifies users, and maintains all user information. In addition, the Subscriber Administrator of an MTF will be able to view and access all compliance assessments within their Subscription. There can only be one Subscriber Administrator for a given Subscription.

The Subscriber Administrator may also set up a compliance assessment for Lead Users by adding a new gap analysis and assigning the project to a Lead User.

The TMA HIPAA Support Center will establish Subscriber Administrator accounts for each designated MTF. The Subscriber Administrator for each MTF will then have the responsibility of establishing accounts for Lead Users and Regular Users at the MTF.

Only Subscriber Administrators can access the Admin window.

### 1.5.2 Lead Users

Lead Users are generally high-level managers that serve in positions such as HIPAA Project Director, Compliance Officer, or Privacy/Security Officer.

Lead Users establish compliance assessments, run reports, and generate project plans (for downloading into Microsoft Project or Excel file). All reports and outputs will be based on the particular assessments that the Lead User has set up.

Lead Users assign HIPAA Requirements to Regular Users for compliance assessments; add or remove team members to a compliance assessment; and “lock” a compliance assessment to prevent any further modifications. Lead Users have access to all information in their compliance assessments and are able to make changes to them. (Lead Users will be able to perform the functions of a Regular User on another Lead User’s compliance assessment. In this situation, the Lead User will only have the privileges of a Regular User.) Lead Users may access the HIPAA Policies and Procedures Module of the software and will be able to download policy templates to reference.

### 1.5.3 Regular Users

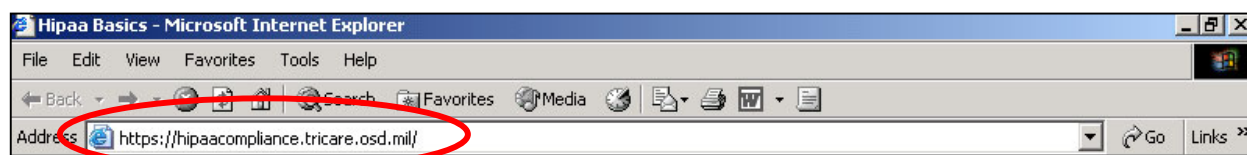
Regular Users are typically subject matter experts in specific areas or assistants to the Lead Users and affiliated with HIPAA work groups. Regular Users have the most basic access to the HIPAA BASICS™ application. Lead Users assign Requirement Questions to the Regular Users as part of a compliance assessment. Regular Users answer only the Requirements Questions to which they are assigned. However, they may view the work of other users assigned to the same compliance assessment.

## 2.0 ACCESSING HIPAA BASICS™

HIPAA BASICS™ is an online application, which can be accessed from any networked location via a Web browser and login information.

To login to the HIPAA BASICS™ application:

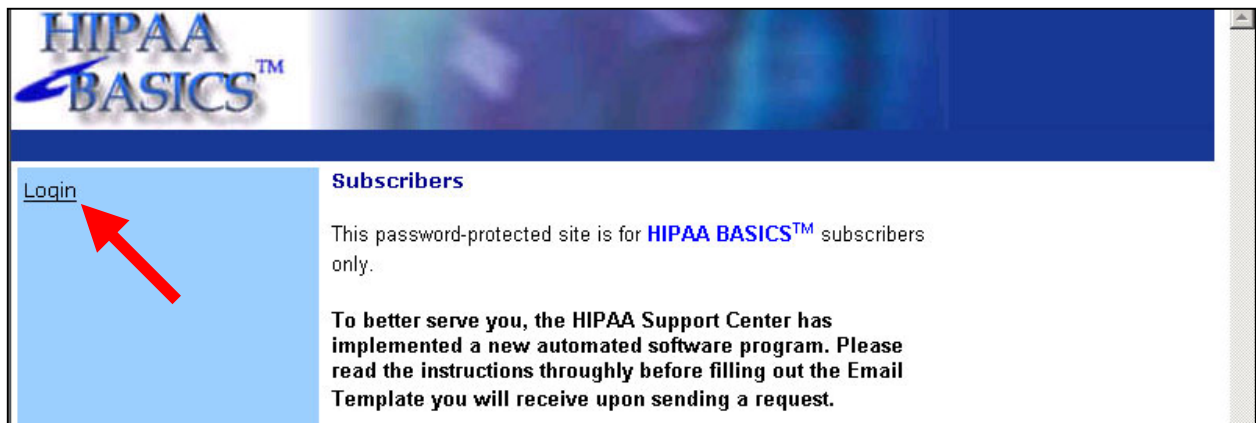
1. Enter the URL for HIPAA BASICS™ into the Web browser,  
 [s://hipaacompliance.tricare.osd.mil/](https://hipaacompliance.tricare.osd.mil/).



**HIPAA BASICS™ URL**

The Login link will appear.

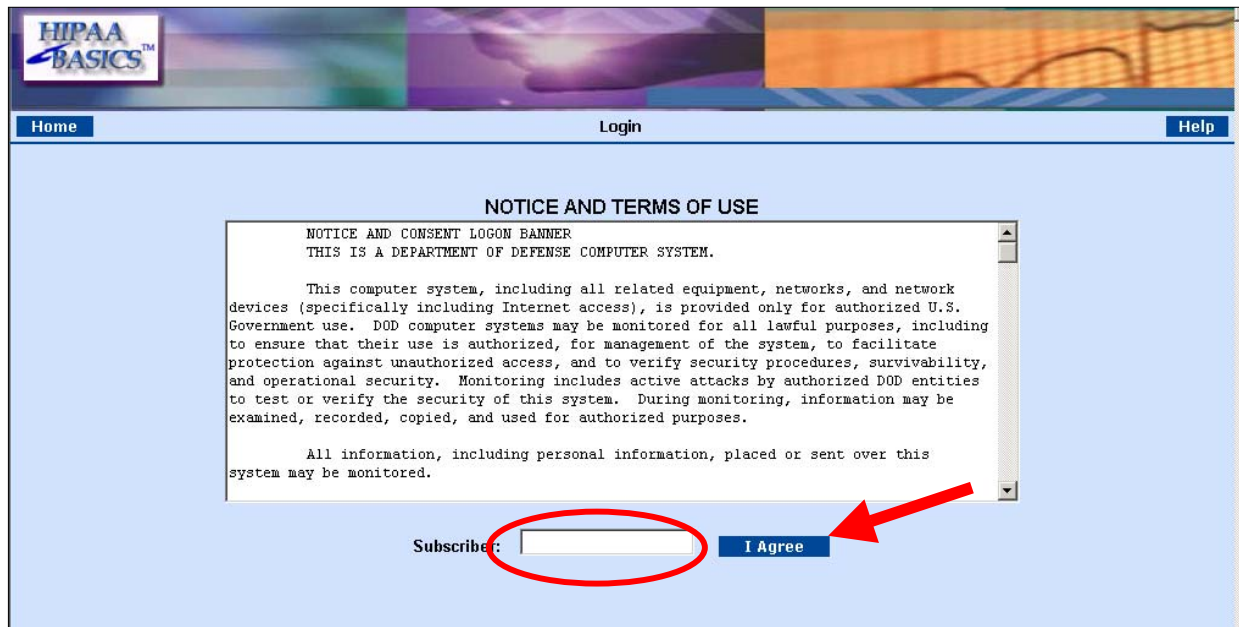
2. Select the **Login** link from the application menu.



Login window

The Subscriber Login window will appear.

3. Enter the name of the **Subscriber** into the text field and click on the **I Agree** button.



Subscriber login window

The User ID and password login window will appear.

4. Enter the **User ID** and **Password** for your account and click on the **Login** button.

*Note: Refer to the password requirements in Section 1.3.*

User ID and password login window

The main menu screen will display.

## 2.1 Main Menu Screen

The main menu screen provides you with access to all HIPAA BASICS™ modules within your Subscription. The main screen is composed of three main parts: the title menu, the application menu, and the application window.

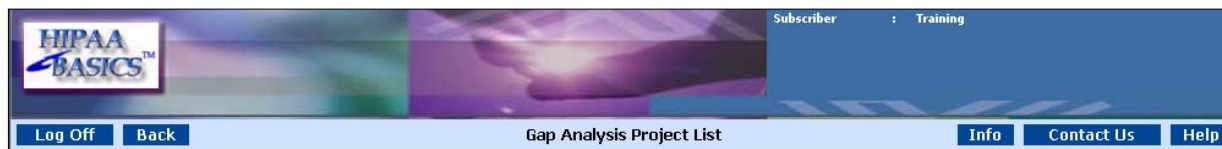
Answer	Assign	Data Collection Date	Gap ID	Rel	Edit	Report	Status
TRAINING	<a href="#">Subscriber Administrator</a>		775	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>
TRAINING	<a href="#">Subscriber Administrator</a>	3/15/2002	MHS Samp xx.1	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>
TRAINING	<a href="#">Subscriber Administrator</a>	2/17/2004	DEMO GAP PREVIOUS VERSION	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>
TRAINING	<a href="#">Gail Brown</a>	3/15/2004	MHS Samp xx.2	3			
TRAINING	<a href="#">Subscriber Administrator</a>	5/14/2004	DEMO GAP	4	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>

Main menu screen



## 2.1.1 Title Menu

The title menu contains navigational buttons and general information on HIPAA BASICS™, as well as, contact information. The title menu lists the application name, current Subscriber, navigational buttons, and contact/resource buttons.



Title menu

### 2.1.1.1 Navigational Buttons



The **Logoff** button must be used whenever you wish to terminate a HIPAA BASICS™ session. If you do not use this button, you will NOT be able to log back into the system immediately. If a session is improperly ended, the system will lock you out for 20 minutes. In order to avoid this occurrence, please make sure that you use the **Logoff** button once your session has ended. For security purposes, you cannot be logged into more than one HIPAA BASICS™ session simultaneously.

The **Menu** button should be used if you wish to be directed to the HIPAA BASICS™ welcome page. The menu button always resides in the title menu, with exception to when you are currently on the welcome page.

### 2.1.1.2 Contact/Resource Buttons



The **Info** button will provide you with any new information and material related to the HIPAA BASICS™ tool. Frequently Asked Questions (FAQs) may be listed as well as other relevant HIPAA BASICS™ information.

The **Contact Us** button can be used if you wish to send an email to the TMA HIPAA Support Center.

The **Help** button is a quick reference for common uses of the HIPAA BASICS™ application. Depending on your location within the tool, the **Help** feature will provide you with information about the current screen.

### 2.1.2 Application Menu

The application menu consists of the operational modules and contains the core operational functions of the application. Depending on the module selected (i.e. “Users”, “Gap Analysis Project List”, “Policies and Forms”, and “Admin”), users will be presented with a list of activities for performing administrative functions and operational functions.



### 2.1.3 Application Window

The application window provides users with access to the data contained within the application modules.

Baseline Administrative Simplification Integrated Compliance Solution							
Answer	Assign	Data Collection Date	Gap ID	Rel	Edit	Report	Status
<a href="#">TRAINING</a>	<a href="#">Subscriber Administrator</a>		775	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>
<a href="#">TRAINING</a>	<a href="#">Subscriber Administrator</a>	3/15/2002	MHS Samp xx.1	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>
<a href="#">TRAINING</a>	<a href="#">Subscriber Administrator</a>	2/17/2004	DEMO GAP PREVIOUS VERSION	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>
<a href="#">TRAINING</a>	<a href="#">Gail Brown</a>	3/15/2004	MHS Samp xx.2	3			
<a href="#">TRAINING</a>	<a href="#">Subscriber Administrator</a>	5/14/2004	DEMO GAP	4	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>

## 2.2 Demo Gap

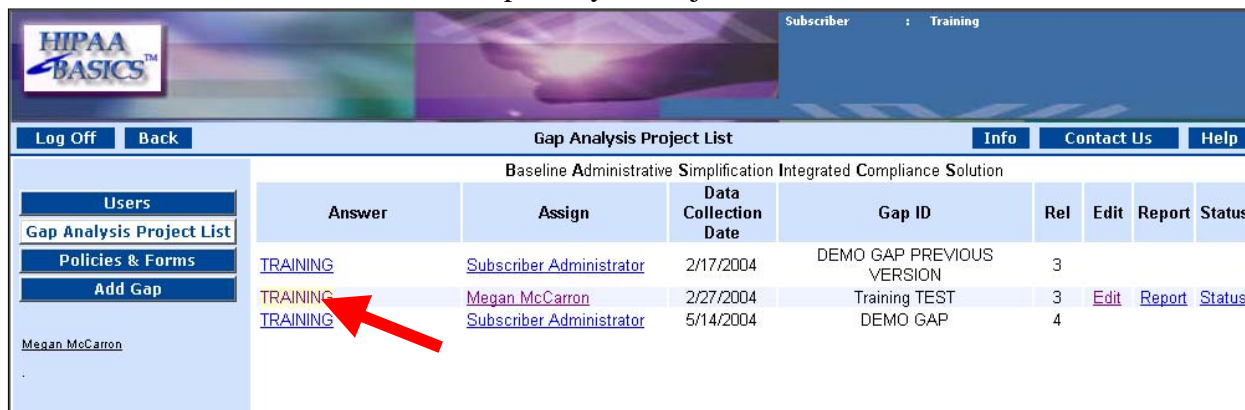
The best way to get started is to login and use the DEMO GAP. This is an assessment (GAP Analysis) that every user will see and have access to. The DEMO GAP is free to experiment with. It will not count toward a limit of assessments set by the License Pack, nor will it be a real assessment. It is meant as a learning tool. You can select any of the hyperlinks to familiarize yourself with the tool and explore the different modules.

### 3.0 ANSWERING REQUIREMENTS AND TASKS

Answering requirements is a function that can be performed by all user levels. As a Lead User you may have to assist members of your Gap Analysis team with completing Requirement Questions. Each requirement is broken down into supporting tasks. There can be up to 20 tasks for each requirement. In order to complete these Requirement Questions, you will need to use the following procedures.

To answer requirements and tasks:

1. Select the **Answer** link from the Gap Analysis Project List window.




Answer	Assign	Data Collection Date	Gap ID	Rel	Edit	Report	Status
<a href="#">TRAINING</a>	<a href="#">Subscriber Administrator</a>	2/17/2004	DEMO GAP PREVIOUS VERSION	3			
<a href="#">TRAINING</a>	<a href="#">Megan McCarron</a>	2/27/2004	Training TEST	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>
<a href="#">TRAINING</a>	<a href="#">Subscriber Administrator</a>	5/14/2004	DEMO GAP	4			

Gap Analysis Project List window

The Requirements and Gap Answers window will display.

2. Sort the Requirement Questions by HIPAA Rule, Functional Area, or Category.
3. Select your name from the **Assigned to** drop-down box in order to identify the Requirement Questions that are assigned to you.



#	Requirement Question	Assigned to
107	A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and respond to suspected or known security incidents; (2) mitigate harmful effects of security incidents that are known to the covered entity; and (3) document security incidents and their outcomes (R).	Megan McCarron
117	Information Access Management through policies and procedures for authorizing access to electronic protected health information that are consistent with HIPAA Privacy Standards, is implemented.	Megan McCarron
123	Procedures for guarding against, detecting, and reporting malicious software are implemented (A).	Megan McCarron
124	Log-in Monitoring procedures for monitoring log-in attempts and reporting discrepancies are implemented (A).	Megan McCarron
126	Security Incident Procedures and policies to address security incidents are implemented.	Megan McCarron
127	Response and Reporting procedures are in place to (1) identify and respond to suspected or known security incidents; (2) mitigate harmful effects of security incidents that are known to the covered entity; and (3) document security incidents and their outcomes (R).	Megan McCarron
129	Ensure that a Data Backup Plan with procedures to create and maintain retrievable exact copies of electronic protected health information are established and implemented as needed (R).	Megan McCarron
131	Procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode are established (and implemented as needed) (R).	Megan McCarron
133	An Applications and Data Criticality Analysis to assess the relative criticality of specific applications and data in support of other contingency plan components is implemented (A).	Megan McCarron

Requirements and Gap Answers window

A list of the Requirement Questions that are assigned to you will appear on the Requirements and Gap Answers window.

4. Select a **Requirement Question** link from the list of assigned requirements.

**HIPAA BASICS™**

Subscriber : Training  
Data Collection Date : 2/27/2004  
Project Start :  
Gap ID : Training TEST (RELEASE 3)  
Lead User : Megan McCarron  
Target Completion :

Log Off Menu Back Requirements and Gap Answers Help

☒ HIPAA Rule ☐ Functional Area ☐ Category

Security Standards Assigned to Megan McCarron

#	Requirement Question
107	<a href="#">A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.</a>
117	<a href="#">Information Access Management through policies and procedures for authorizing access to electronic protected health information, that are consistent with HIPAA Privacy Standards, is implemented.</a>
123	<a href="#">Procedures for guarding against, detecting, and reporting malicious software are implemented (A).</a>
124	<a href="#">Log-in Monitoring procedures for monitoring log-in attempts and reporting discrepancies are implemented (A).</a>
126	<a href="#">Security Incident Procedures and policies to address security incidents are implemented.</a>
127	<a href="#">Response and Reporting procedures are in place to (1) identify and respond to suspected or known security incidents; (2) mitigate harmful effects of security incidents that are known to the covered entity; and (3) document security incidents and their outcomes (R).</a>
129	<a href="#">Ensure that a Data Backup Plan with procedures to create and maintain retrievable exact copies of electronic protected health information are established and implemented as needed (R).</a>
131	<a href="#">Procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode are established (and implemented as needed) (R).</a>

**Requirements and Gap Answers window**

The Requirement Tasks window will display.

5. Scroll down to the bottom of the Requirement Tasks window.

*Note: Lead Users have the ability to change the applicability of each task. This is done by removing the check for those tasks that are not applicable. Follow the guideline set forth by your Service for selecting the applicability of tasks.*

6. Select the link for the task that you will answer.

107.01	Complete	<a href="#">The administrative policies and procedures used to meet this requirement are documented.</a>	<input checked="" type="checkbox"/>
107.02	Complete	<a href="#">The principle of least privilege is addressed. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.03	Complete	<a href="#">Separation of duties is addressed. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.04	Complete	<a href="#">The required qualifications for each security management role are included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.05	Complete	<a href="#">An information security official role or equivalent is included.</a>	<input checked="" type="checkbox"/>
107.06	Not Answered	<a href="#">An internal auditor role or equivalent is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.07	Not Answered	<a href="#">A technical security management role is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.08	Not Answered	<a href="#">A personnel clearance framework is established or referenced.</a>	<input checked="" type="checkbox"/>
107.09	Not Answered	<a href="#">A physical security management role is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.10	Not Answered	<a href="#">A hierarchy of security management roles is specified. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.11	Not Answered	<a href="#">The procedures for nominating candidates to fill each role are outlined. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.12	Not Answered	<a href="#">The procedures for selecting a candidate for each defined security management role are outlined. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.13	Not Answered	<a href="#">The duration an individual is assigned to a given role is indicated. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.14	Not Answered	<a href="#">An administrative security management role is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.15	Not Answered	<a href="#">A description for each of security management team member's responsibilities and duties is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.16	Not Answered	<a href="#">A security management plan that addresses prevention, detection, containment, and correction of security violations is included.</a>	<input checked="" type="checkbox"/>
107.17	Not Answered	<a href="#">The security management plan includes all of the workforce, including those working from home.</a>	<input checked="" type="checkbox"/>
107.18	Not Answered	<a href="#">A compliance program is included in the security management plan.</a>	<input checked="" type="checkbox"/>
107.19	Not Answered	<a href="#">A training program is included in the security management plan.</a>	<input checked="" type="checkbox"/>
107.20	Not Answered	<a href="#">Processes to ensure reasonableness and appropriateness of security controls selected, considering risk analyses and factors specific to the organization (e.g., size, environment, operating changes, configuration) are included.</a>	<input checked="" type="checkbox"/>
<input type="checkbox"/> All Complete / Not Complete		<input type="radio"/> Applicable <input type="radio"/> Not Applicable <input checked="" type="radio"/> All	<input type="checkbox"/> On / Off

**Requirement Tasks window**

The Task Notes window will display.

7. Review the Regulatory Requirement and Requirement Intro.

8. Enter a Task Note

*Note: Task Notes are required by TMA. Task notes should identify the policy/document that was used to support the particular task.*

9. Click on the **Update** button.

The screenshot shows the 'Task Notes' window. At the top, there is a header bar with 'Log Off', 'Menu', 'Back', 'Task Notes', and 'Help' buttons. Below this is a table with the following content:

<b>HIPAA Rule</b>	Security Standards
<b>Functional Area</b>	Information Technology
<b>Project Category</b>	VI: Security Management Process
<b>Requirement Question</b>	107: A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.
<b>Regulatory Authority</b>	A covered entity must implement Administrative Safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains, or transmits. The safeguards must protect against reasonably anticipated threats or hazards to the security and integrity of such information. They must also protect against any reasonably anticipated uses and disclosures of such information that are not permitted or required. The approach is flexible. In deciding which security measures to use, a covered entity must take into account a variety of factors, including size, complexity and capabilities of the covered entity, cost, technical infrastructure and capabilities, and probability and criticality of potential risks. [164.308 (a)(1)(i); in accordance with § 164.306(a)(b)]
<b>Requirement Intro</b>	Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. An implementation requirement standard of the administrative safeguards includes a documented and well communicated Security Management Process is important as it enforces the formal analysis and assessment of risks as well as audits and sanctions. Being informed and prepared is critical for success. The security management process accomplishes this in an ever-changing security risk environment. Security standards establish a minimum level of security that covered entities must meet.

Below the table, there is a section for 'TaskID' (107.01), 'Requirement Test' (The administrative policies and procedures used to meet this requirement are documented), and 'Task Notes' (completed on 3/31/04). A red box highlights the 'Task Notes' text area. Below the text area is an 'Update' button, which is pointed to by a red arrow.

**Task Notes window**

The Task Notes section will be saved.

10. Click on the **Back** Button to return to the Requirement Tasks window.

11. Locate the Requirement task that you just completed.

12. Select the status of the task from the drop down box.

*Note: You can select **Complete** or **Not Complete**.*

13. Click on the **Update** button to save your work.

*Note: You will have to repeat the process of answering a task and entering a note for all tasks related to a given requirement. Once you have answered Complete for all related tasks, you will be compliant with that requirement.*




107.01	Complete	<a href="#">Administrative policies and procedures used to meet this requirement are documented.</a>	<input checked="" type="checkbox"/>
107.02	Not Complete	<a href="#">The principle of least privilege is addressed. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.03	Complete	<a href="#">Separation of duties is addressed. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.04	Complete	<a href="#">The required qualifications for each security management role are included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.05	Complete	<a href="#">An information security official role or equivalent is included.</a>	<input checked="" type="checkbox"/>
107.06	Not Answered	<a href="#">An internal auditor role or equivalent is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.07	Not Answered	<a href="#">A technical security management role is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.08	Not Answered	<a href="#">A personnel clearance framework is established or referenced.</a>	<input checked="" type="checkbox"/>
107.09	Not Answered	<a href="#">A physical security management role is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.10	Not Answered	<a href="#">A hierarchy of security management roles is specified. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.11	Not Answered	<a href="#">The procedures for nominating candidates to fill each role are outlined. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.12	Not Answered	<a href="#">The procedures for selecting a candidate for each defined security management role are outlined. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.13	Not Answered	<a href="#">The duration an individual is assigned to a given role is indicated. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.14	Not Answered	<a href="#">An administrative security management role is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.15	Not Answered	<a href="#">A description for each of security management team member's responsibilities and duties is included. [OPTIONAL]</a>	<input checked="" type="checkbox"/>
107.16	Not Answered	<a href="#">A security management plan that addresses prevention, detection, containment, and correction of security violations is included.</a>	<input checked="" type="checkbox"/>
107.17	Not Answered	<a href="#">The security management plan includes all of the workforce, including those working from home.</a>	<input checked="" type="checkbox"/>
107.18	Not Answered	<a href="#">A compliance program is included in the security management plan.</a>	<input checked="" type="checkbox"/>
107.19	Not Answered	<a href="#">A training program is included in the security management plan.</a>	<input checked="" type="checkbox"/>
107.20	Not Answered	<a href="#">Processes to ensure reasonableness and appropriateness of security controls selected, considering risk analyses and factors specific to the organization (e.g., size, environment, operating changes, configuration) are included.</a>	<input checked="" type="checkbox"/>
<input type="checkbox"/> All Complete / Not Complete		<input type="radio"/> Applicable <input type="radio"/> Not Applicable <input checked="" type="radio"/> All	<input type="checkbox"/> On / Off
ID	Status	Requirement Test	Applicability
		<a href="#">Update</a>	Assigned to : Megan McCarron

### Requirement Tasks window

The status of the task will be saved.

14. Select the **Requirement Question** link on the Requirement Tasks window to enter a Requirement Note.



Subscriber : Training  
 Data Collection Date : 2/27/2004  
 Project Start :  
 Gap ID : Training TEST (RELEASE 3)  
 Lead User : Megan McCarron  
 Target Completion :

Please click on Update to save changes...

[Log Off](#)
[Menu](#)
[Back](#)
[Requirement Tasks](#)
[Help](#)

**HIPAA Rule** Security Standards

**Functional Area** Information Technology

**Project Category** VI: Security Management Process

**Requirement Question** 107: A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.

**Regulatory Authority** A covered entity must implement Administrative Safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains, or transmits. The safeguards must protect against reasonably anticipated threats or hazards to the security and integrity of such information. They must also protect against any reasonably anticipated uses and disclosures of such information that are not permitted or required. The approach is flexible. In deciding which security measures to use, a covered entity must take into account a variety of factors, including size, complexity and capabilities of the covered entity, cost, technical infrastructure and capabilities, and probability and criticality of potential risks. [164.308 (a)(1)(i); in accordance with § 164.306(a)(b)]

**Requirement Intro** Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. An implementation requirement standard of the administrative safeguards includes a documented and well communicated Security Management Process is important as it enforces the formal analysis and assessment of risks as well as audits and sanctions. Being informed and prepared is critical for success. The security management process accomplishes this in an ever-changing security risk environment. Security standards establish a minimum level of security that covered entities must meet.

[Update](#)
Assigned to : Megan McCarron

ID	Status	Requirement Test	Applicability
<input type="checkbox"/> All Complete / Not Complete		<input type="radio"/> Applicable <input type="radio"/> Not Applicable <input checked="" type="radio"/> All	<input type="checkbox"/> On / Off

### Requirement Tasks window

The Requirement Notes window will display.

15. Enter a Requirement Note.

16. Click on the **Update** button.

**HIPAA BASICS™**  
Please click on Add/Update to save changes...

**Log Off** **Menu** **Back** **Requirement Notes** **Help**

**HIPAA Rule** Security Standards  
**Functional Area** Information Technology  
**Project Category** VI: Security Management Process  
**Requirement Question** 107: A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.  
**Regulatory Authority** A covered entity must implement Administrative Safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains, or transmits. The safeguards must protect against reasonably anticipated threats or hazards to the security and integrity of such information. They must also protect against any reasonably anticipated uses and disclosures of such information that are not permitted or required. The approach is flexible. In deciding which security measures to use, a covered entity must take into account a variety of factors, including size, complexity and capabilities of the covered entity, cost, technical infrastructure and capabilities, and probability and criticality of potential risks. [164.308 (a)(1)(i); in accordance with § 164.306(a)(b)]  
**Requirement Intro** Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. An implementation requirement standard of the administrative safeguards includes a documented and well communicated Security Management Process is important as it enforces the formal analysis and assessment of risks as well as audits and sanctions. Being informed and prepared is critical for success. The security management process accomplishes this in an ever-changing security risk environment. Security standards establish a minimum level of security that covered entities must meet.

**Requirement Notes**

In process. Completed 5 tasks

**Update**

Requirement Notes window

## 4.0 TECHNICAL SUPPORT

This section provides contact information and covers some of the usability issues that you may encounter within the HIPAA BASICS™ application.

### 4.1 System Maintenance

HIPAA BASICS™ users will be notified before system maintenance is performed on the BASICS™ system. The TMA HIPAA Support Center operates from 8 am to 5 pm EST Monday – Friday and can be reached by email at [hipaasupport@tma.osd.mil](mailto:hipaasupport@tma.osd.mil).

## 4.2 Information Updates

The **Info** link provides information and updates to all users within the application. Frequently Asked Questions (FAQs) are listed, as well as other relevant HIPAA BASICS™ information as changes in the regulation or in the HIPAA BASICS™ application occur. This page is updated by the TMA HIPAA Support Center regularly.

System Updates are communicated to the MTF Subscriber users by email.

Additional help can be requested using the **Contact Us** link. This will allow you to send an email to the TMA HIPAA Support Center.

The TMA HIPAA Support Center will respond to requests within TWO BUSINESS DAYS.

## 4.3 Version Upgrades

HIPAA BASICS™ will be updated periodically. This occurs when a HIPAA regulatory change occurs. Once a Notice of Proposed Rule Making (NPRM) HIPAA Rule is finalized the application will be updated and a new version is released. Users will be notified in advance, both on upcoming regulatory changes as well upcoming updates to the application.

Information about the New Release can be found at the Info page on the Main Menu.

The Release or Version number that is associated with a Gap Analysis is displayed in the **Rel** column on the Main Menu.

Note: You can only upgrade to the next version release, i.e. from version 2 to version 3, not from version 1 to version 3. Therefore, you must be sure to upgrade every time there is a new release.



Answer	Assignments	Data Collection Date	Gap ID	Rel	Edit	Report	Status Report	Gap Status
<a href="#">TRAINING</a>	<a href="#">Megan McCarron</a>	2/27/2004	Training TEST	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>	
<a href="#">TRAINING</a>	<a href="#">Alec Karry</a>	2/15/2004	Sample Gap ID	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>	
<a href="#">TRAINING</a>	<a href="#">Alec Karry</a>	2/15/2004	XXX - GAP	3	<a href="#">Edit</a>	<a href="#">Report</a>	<a href="#">Status</a>	

Gap Analysis Project List window

## 4.4 TMA HIPAA SUPPORT CENTER

TMA HIPAA Support Center staff members are responsible for creating/ setting up new Subscribers, managing License Packs (but not creating), and assisting the Subscriber Administrators by email. Support Center staff has the right to log in as a Subscriber Administrator in order to provide support and/or replicate a reported problem. Support Center staff communicates with the users of the system via emails that can be sent from within the HIPAA BASICS™ application.

You can contact the TMA HIPAA Support Center at: [hipaasupport@tma.osd.mil](mailto:hipaasupport@tma.osd.mil)

Hours of operation: Monday – Friday, 8:00 am – 5:00 pm Eastern Standard Time (EST).



## 5.0 GLOSSARY

To facilitate clarity the following terms will be used throughout the document and are defined as follows:

**Assessment:** An Assessment is a gap analysis undertaken to review compliance status. A Lead User or Subscriber Administrator within a Subscription conducts an Assessment.

**Category:** Project Categories are proprietary to HIPAA BASICS™. They serve as filters for the **Requirements** of the different **HIPAA Rules**. Categories also organize the MS Project plan that is generated from a particular assessment in which gaps were identified.

**Chief Privacy Official (CPO):** The Privacy Official formally assigned the responsibility for a covered entity's compliance with the Privacy rule. Large entities may have additional privacy officials charged with assisting privacy implementation in different facilities of the entity. For example, a large Military Treatment Facility (MTF) entity (composed of a medical center and outlying facilities) may have more than one "privacy official" subordinate, for implementation actions. A smaller entity, such as a community hospital model MTF may have only a single Privacy Official. The CPO may also be known as the "Chief Privacy Officer" or "Command Privacy Officer".

**Covered Entity:** A Covered Entity is a regulatory term used in HIPAA Administrative Simplification. A covered entity is defined as a health plan, clearinghouse, or provider.

**HIPAA BASICS™:** A commercial off-the-shelf (COTS) web-based application designed to assess and track HIPAA compliance within a healthcare care delivery system or health plan, i.e., a covered entity. HIPAA BASICS™ comprehensively assesses HIPAA compliance as it covers all **HIPAA Rules**.

**HIPAA Rule:** One the five Rules that make up the Health Insurance Portability and Accountability Act of 1996 Administrative Simplification. HIPAA BASICS™ displays only current final Rules. If there has never been a final rule, the NPRM Rule (Notice of Proposed Rule Making) will be displayed.

**MTF:** Military Treatment Facility. "MTF" is an entity that is defined by assignment of compliance responsibility, not by location or size; It is synonymous with the covered entity for which the **Chief Privacy Official** is responsible. An MTF can be as small as a community hospital and as large as a medical center with multiple clinics and/or other ancillary facilities.

**MTF-Level Privacy Assessment:** A term used in this CONOPS to label that one particular assessment that is specifically recommended to cover the Privacy compliance status of the MTF (as defined above) and forms the basis for remediation efforts as well as future tracking.

**NPRM (Notice of Proposed Rule Making):** The preliminary form in which HIPAA Rules are released before they become final. NPRMs represent "rough drafts" of HIPAA Rules.

**New Release:** An updated version of HIPAA BASICS™ with new content that reflects some regulatory change. For example, a New Release would be produced when a HIPAA Rule moved from NPRM status to its final rule.

**New Version:** A feature of HIPAA BASICS™ that allows the creation of a duplicate (copy) of an existing assessment so that compliance status within that assessment can be updated without destroying the audit trail. This feature allows a **Lead User** to show changes in compliance status while leaving the original assessment record intact and without constructing a new assessment from scratch.

**Privacy Team:** A workgroup that is assigned organizational planning and remediation responsibilities to accomplish MTF compliance with the Privacy Rule. The CPO typically organizes and leads this team. At a minimum, members of the Privacy Team include HIPAA BASICS™ Lead and Regular Users (see **Team Assigned**). The team can include other MTF/facility staff as deemed necessary by the **CPO**.

**Requirement:** A term used in HIPAA BASICS™ that refers to a regulatory standard of a HIPAA Rule.

**Subscriber:** A HIPAA BASICS™ term that refers to a group of application end users that collaborate on HIPAA assessments and tracking. A Subscription always includes the following three types of HIPAA BASICS™ users: Subscriber Administrator, Lead User and Regular User. There will be one Subscription for each **MTF** (as defined above) in the MHS.

**Team Assigned:** A term used within HIPAA BASICS™. It refers to a team of HIPAA BASICS™ users within a Subscription who work jointly on an assessment. Each assessment has its own distinct team of users.

**TMA:** TRICARE Management Activity (TMA), the customer and part of MHS that obtains a license to use the HIPAA BASICS™ application on its servers or network.

**Upgrade to New Version:** A feature in HIPAA BASICS™ that allows a user to upgrade a previous assessment to a New Release of the application.